Označenie

1. $rand$ – vráti náhodný real $y \in < 0, 1)$
2. $grand(a, b)$ – vráti náhodný real $y \in < a, b), a, b \in \mathcal{R}$
3. $irand(i, j)$ – vráti náhodné cele $y \in < i, j >, i, j \in \mathcal{Z}$
4. $brand$ – „hodí mincou“ a vráti 0 alebo 1.

Poznámka Pomocou hociktorej procedúry (1) – (4) je možné zostrojiť ostatné:

- $grand(a, b) = a + (b - a) * rand$
- $irand(i, j) = \lfloor grand(i, j + 1) \rfloor$
- $brand = irand(0, 1)$
- $$brand = \begin{cases} 0 & rand \text{vrátí} y < \frac{1}{2} \\ 1 & \text{inak} \end{cases}$$

```
procedure rand
vykonaj brand r-krat s vysledkami b_1, b_2, ... b_r (b_i \in {0,1} \forall i)
return y=0.b_1b_2...b_r (real.y\in<0,1) v bin. tvare).
end;
```

Definícia *Pravdepodobnostný algoritmus* akceptuje jazyk $L \in \Sigma^*$ s chybou $\varepsilon (0 < \varepsilon < \frac{1}{2})$ ak $\forall x \in \Sigma^*$ platí: Pravdepodobnosť toho, že A akceptuje $x \notin L$ (zamietne $x \in L$) je $\leq \varepsilon$ (t.j. A akceptuje $x \in L$ (resp. zamietne $x \notin L$) s pravdepodobnosťou $\geq 1 - \varepsilon$).

Príklad Nech A používa $brand$.

Strom pravdepodobnostného výpočtu A x vrcholy – volania $brand$; a – akceptuj, z – zamietni.

Do konkrétneho listu s hĺbkou l sa$A$ dostane s pravdepodobnosťou $2^{-l} \Rightarrow$ A akceptuje s pravdepodobnosťou $2^{-2} + 2^{-3} + 2^{-4} = 7/16$, zamietne s $2^{-2} + 2^{-2} + 2^{-4} = \frac{9}{16}$.

Definícia (bounded-error probabilisic polynomial)

$$BPP = \{L \mid \exists \text{pravdepodobnostný polynomiálny algoritmus akceptujúci s chybou} \leq \varepsilon (0 < \varepsilon < \frac{1}{2}\}$$

Veta $P \subseteq BPP \subseteq PSPACE$.

Dôkaz $P \subseteq BPP$ – zrejmé. Nech $L \in BPP$, nech A je pravdepodobnostný algoritmus akceptujúci L v polynomiálnom čase $p(x)$ s chybou ε. Nech M je deterministický Turingov stroj s pamäťou $p(n)$, ktorý na vstupe x:

- na jednej z pracovných pások postupne generuje všetky binárne postupnosti dĺžky $\leq p(n)$.
- po vygenerovaní každdej postupnosti stroj M simuluje výpočet algoritmu A na vstupe x s hodnotami *brand* určenýmmi vygenerovanou postupnosťou, pričom existuje ignoruje postupnosti s nevhodným počtom volaní *brand*.
- M priebežne počíta pravdepodobnosť toho, že A akceptuje x.
- M akceptuje x, ak A akceptuje x s pravdepodobnosťou $\geq 1 - \varepsilon$, inak M zamietne x. Z toho vyplýva, že $L \in PSPACE$.

Dôsledok

$$P \subseteq \left\{ \begin{array}{c} NP \\ BPP \end{array} \right\} \subseteq PSPACE$$

Poznámka

- nie je známe, či $P = BPP$ alebo či $BPP = PSPACE$
- nie je známy žiaden vzťah NP a BPP

Veta (o vylepšovaní) Nech A je pravdepodobnostný algoritmus akceptujúci $L \subseteq \Sigma^*$ v čase $T(n)$ s chybou ε, $(0 < \varepsilon < \frac{1}{2})$. Potom $\forall \varepsilon' (0 < \varepsilon' < \varepsilon$ existuje pravdepodobnostný algoritmus A' akceptujúci L v čase $O(T(n))$ s chybou ε'.

Dôkaz Algoritmus A': A' akceptuje (zamietne) vstup x, ak spomedzi m náhodne vybraných výpočtov A na x (A' ich vyberie a simuluje) je počet akceptujúcich (zamietajúcich) väčší než počet zamietajúcich (akceptujúcich). m je nepárne číslo, t.j. $\frac{1}{2}(4(1-\varepsilon)\varepsilon)^{m/2} \leq \varepsilon'$. (Také m existuje, lebo $0 < 4(1-\varepsilon)\varepsilon = 4(\frac{1}{2}+\alpha)(\frac{1}{2}-\alpha) = 1 - 4\alpha^2 < 1$ pre $0 < \varepsilon < \frac{1}{2}$ a $O < \alpha' \frac{1}{2} - \varepsilon < \frac{1}{2}$). Pravdepodobnosť chyby A' na x je $\leq \frac{1}{2}(4(1-\varepsilon)\varepsilon)^{m/2}$, lebo:

Prípad 1 $x \in L$ Nech ε_x je pravdepodobnosť toho, že náhodne vybraný výpočet A na x je zamietajnúci, teda $O \leq \varepsilon_x \leq \varepsilon$ a $1 - \varepsilon_x =$ pravdepodobnosť toho, že náhodne vybraný výpočet A na x je akceptujúci.

Príklad Nech p je pravdepodobnosť toho, že postupnosť 5 náhodne vybraných výpoštov A na x je tvaru a, z, z, a, z (a – akceptujúci, z – zamietajúci):

$$p = (1 - \varepsilon_x)\varepsilon_x\varepsilon_x(1 - \varepsilon_x)\varepsilon_x = (1 - \varepsilon_x)^2\varepsilon_x^3$$

. $\binom{5}{2}$ = počet postupností dĺžky 5 s dvomi „a“ a tromi „z“. Teda $\binom{5}{2}(1-\varepsilon_x)^2\varepsilon_x^3$ = pravdepodobnosť toho, že postupnosť 5 náhodných výpočtov A na x obsahuje 2 akceptačné a 3 zamietajúce výpočty.

$$\sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j} (1-\varepsilon_x)^j \varepsilon_x^{m-j}$$

Pravdepodobnosť toho, že posledných m náhodne vybraných výpočtov A na x obsahuje $\leq \lfloor m/2 \rfloor$ akceptačných výpočtov (t.j. obsahuje viac zamietajúcich než zamietajúcich výpočtov) = pravdepodobnosť toho, že A' zamietne $x \in L$ = pravdepodobnosť chyby A' na $x \in L$.

Prípad 1a $\varepsilon_x = 0 \Rightarrow \sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j}(1-\varepsilon_x)^j \varepsilon_x^{m-j} = 0 < \frac{1}{2}(4(1-\varepsilon)\varepsilon)^{m/2}$.

Prípad 1b $\varepsilon_x > 0 \Rightarrow 1 < \frac{1-\varepsilon_x}{\varepsilon_x}$ (lebo $O < \varepsilon_x \leq \varepsilon < \frac{1}{2} \Rightarrow \sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j}(1-\varepsilon_x)^j \varepsilon_x^{m-j} \leq \sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j}(1-\varepsilon_x)^j \varepsilon_x^{m-j} \underbrace{\left(\frac{1-\varepsilon_x}{\varepsilon_x}\right)^{m/2-j}}_{>1} = \underbrace{\sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j}}_{2^m/2 = \frac{1}{2}((2^2)^{m/2}} (+ - \varepsilon_x)^{m/2}\varepsilon_x^{m/2} = \frac{1}{2}(2^2(1-\varepsilon_x)\varepsilon_x)^{m/2} \leq \frac{1}{2}(4(1-\varepsilon)\varepsilon)^{m/2}$

Posledná nerovnosť nie je triviálna:

$(1-\varepsilon)\varepsilon = (1-\varepsilon_x)\varepsilon_x + \underbrace{(\varepsilon-\varepsilon_x)}_{\geq 0}\underbrace{(1-\varepsilon-\varepsilon_x)}_{\geq 0} \geq (1-\varepsilon_x)\varepsilon_x$

Príklad 2 $x \notin L$. Dôkaz je podobný prípadu 1. Pravdepodobnosť chyby A' na x je $\leq \frac{1}{2}(4(1-\varepsilon!\varepsilon)^{m/2} \underbrace{\leq \varepsilon'}_{\substack{\text{výber } m \text{ v } A'}} \Rightarrow$ veta.

Dôsledok (dôkazu). Ak pre každé n vykoná A' na každodm vstupe x dĺžky n práve $2n+1$ náhodne vybraných výpočtov A na x, potom A' akceptuje $L \cap \Sigma^n$ v čase $O(nT(n))$ s chybou $\frac{1}{2}(\underbrace{4(1-\varepsilon)\varepsilon}_{<1})^{n+\frac{1}{2}}$